NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

Closing the Real Cybersecurity Talent Gap: The Case for Expanding Federal Cyber Scholarship for Service Programs

By Patrick Gaul
Executive Director
National Technology Security Coalition

When talking about such an important topic as cybersecurity workforce development, it's easy to get lazy. Articles and presentations begin to sound the same, and statistics get quoted through the years without people questioning their source. For example:

- 3.5 million unfilled cybersecurity positions is often mistakenly applied to the US. This is the global cybersecurity talent shortfall. In the US, we do have a shortfall of 3.4 million predicted unfilled technical positions that include all technical fields—not just cybersecurity. People sometimes confuse these two statistics.
- We often hear that the cybersecurity talent shortfall includes all cybersecurity jobs. However, current statistics from Cyberseek show demand is mostly for positions requiring experience—while the current supply of entry-level cybersecurity candidates exceeds demand.
- We often hear that only 11 percent of the cybersecurity workforce are women. It's actually 24 percent—still not great but improved. The 11 percent stat is a much older statistic that doesn't often get updated by journalists, trade publication writers, and speakers.

Repeating these same tired myths, anecdotes, and misunderstood statistics get us nowhere when addressing cybersecurity workforce issues. Do we have a talent shortfall? Yes. But what are the real facts? How will those facts impact a national workforce development strategy? And what should we do to solve the problem?

Because cybersecurity workforce development is such a major focus for both the public and private sectors, we must seek accurate, specific answers and solutions to solve the problem. To meet our goals, we cannot just focus on limited programs or sporadic company initiatives. To impact everyone, we need a national initiative to make workforce development transformational across the country and make the US the global leader in cybersecurity workforce development.

This whitepaper will address:

- Facts about the actual cybersecurity talent gap
- What kind of pipeline we actually need, and why
- The root causes of our talent pipeline issues
- How a cyber scholarship for service program (and related apprenticeship programs) can solve the cybersecurity talent problem—addressing both the quantity and experience of candidates

So, Where's the Real Talent Gap?

Cyberseek is an online tool, grant-funded and supported by the National Initiative for Cybersecurity Education (NICE), that reports on cybersecurity talent demand in real time. They offer data about the supply and demand of cybersecurity jobs in ways that allow a user to segment between different levels of job categories, experience, and geography. When sliced and diced, the data shows us some interesting insights about the real talent gap.

If we look at the numbers superficially, the market is tight. Overall, as of November 13, 2020, we see that there are 1.8 unemployed cybersecurity workers for every one job—which is far below the national average of 3.34 unemployed workers for every one job across the United States. However, let's take a deeper look at the data through the lens of certifications.

Job demand for entry-level cybersecurity professionals

We often hear that the cybersecurity talent shortage applies to all positions. However, Cyberseek shows 3.51 certification holders (as of November 13, 2020) for every job opening requiring an entry-level CompTIA Security+ certification, which focuses on baseline cybersecurity skills. As we can see from this data, there is not a significant demand for such "career starter" professionals. Entry-level candidates, based on this data, will have trouble finding jobs.

Surely, these are still jobs that need to get done, and they give candidates basic skills and experience that form important career building blocks. In the long run, this fresh talent will eventually create a pipeline of more experienced talent that benefits organizations—especially those organizations taking a more strategic look at their workforces. However, the reality in the short term is that the supply of inexperienced talent exceeds the number of current job openings.

Job demand for experienced cybersecurity professionals

When we consider mid-career jobs that require 7-10 years of experience, we start to see a crunch. Then, when considering higher-level certifications, the crunch gets tighter and tighter.

For example, as of November 13, 2020, the number of people with certifications such as CISSP (0.766 holders for every available job requiring this certification), CISA (0.583), and CISM (0.401) are less than the number of job openings.

People with certifications who are advanced in their careers are rare, and the talent shortfall scarcity really lies with these experienced cybersecurity professionals. While entry-level jobs and developmental opportunities are still part of a long-term cybersecurity talent pipeline strategy, we are addressing the wrong problem if we focus too much on people right out of college or who have "career starter" cybersecurity certifications. Instead, we need to focus on the lack of seasoned professionals with 7-10 years of experience.

The military lacks enough people to bridge this talent gap

Many CISOs and cybersecurity leaders often tout higher recruitment of veterans (which is fantastic) as a possible answer. However, the numbers just don't address the problem. Among all the military cyber services (including US Cyber Command), there are about 8,000 service members in the cybersecurity field. Let's say a third will get out of the military over the next 12 months, a third will leave in the next few years, and the other third are career military. While a small talent pool, these candidates can offer valuable mid-career experience to the cybersecurity workforce. But with those low numbers, it's impossible to fill the private sector cybersecurity talent gap—even if all these service members entered the private workforce.

A critical shortage of public sector cybersecurity talent

As of November 13, 2020, there are about 37,000 cybersecurity job openings in the public sector—meaning that about 40 percent of positions are currently unfilled. Critical shortages exist in the public sector largely because the federal government, on the surface, appears to be a less appealing proposition than the private sector. The government generally pays a lower salary than the private sector, the hiring process can be bureaucratic and complicated, and federal agencies can seem much less desirable from a branding perspective compared to flashy private sector companies.

Additionally, Title 5 rules have become ponderous, tediously outdated, and unhelpful in getting the right talent on board. Federal agencies are trying to improve hiring processes through some isolated attempts. For example, a new initiative within DHS called the Cyber Talent Management System has the potential to break through the existing morass as a special hiring authority, but it's meeting with some resistance. Old habits die hard.

The Cyberspace Solarium Commission report states “[The] federal government must reform how it recruits, trains, and educates its workforce to ensure that it has the necessary cybersecurity talent. Shortages in such talent are widespread in both the public and private sectors, and the federal government has a role to play (in partnership with academia and industry) to ‘grow the pie’ of qualified cybersecurity workers, make certain that existing sources of talent are not overlooked, and build the pipelines and career paths that put the right people in the right places for confronting threats from cyberspace.”

The cybersecurity experts and legislators who wrote the report acknowledge not only the public sector cybersecurity shortage and its root issues but also the need for the federal government to play a role in increasing the number of “qualified” workers. Before we examine solutions, it’s useful to understand why we lack such qualified workers—stemming as far back as K-12.

Acknowledging the Root Causes of Cybersecurity Talent Pool Problems

Before we look more closely at the urgency for solutions now, it's worth acknowledging deeper root causes of the overall talent shortage. We will also show that concentrating only on these long-term strategic aspects will not alone help us solve our talent pipeline problems in the short-term.

Lack of cybersecurity evangelization at the K-12 level

Plenty of room still exists for creating more excitement early on for K-12 students around a cybersecurity career path—from encouraging interest in the subject to introducing mentors in the field who connect to kids. It is outside the scope of this whitepaper to fully address this topic, but we acknowledge its importance as a long-term strategy toward getting a broader number of people interested in cybersecurity over the next few decades. Cybersecurity is still a young field relative to many other fields, and so we need to plant seeds now if we are to see fruit later.

However, this is a long-term strategy and it will take decades to see results. Systemic issues must be addressed at deep, deep levels such as stronger STEM education, cybersecurity education training for K-12 teachers, well-designed and funded cybersecurity education programs that include most schools in the United States, and public service marketing and branding that increases awareness and communicates the appeal of a cybersecurity career. While all very important, these aspirational efforts cannot be our primary effort to help with short-term experienced talent shortage needs now and within the next few years.

Academic and HR inflexibility in career paths

Another systemic problem is academic and human resources inflexibility where schools and companies view a cybersecurity degree path in traditional, narrow terms such as a four-year college degree requirement. Cybersecurity career paths get treated the same way HR departments view accounting or business experience—mapping degrees and specific experience exactly to detailed cybersecurity job descriptions. Many CISOs tell the NTSC that a lot of cybersecurity talent is untapped in the marketplace, whether through the absence of candidates with degrees from two-year and trade school programs or candidates with aptitude but untraditional cybersecurity experience.

Obviously, we must push through this problem and find ways to more objectively evaluate potential hires. Degrees and certifications are just one way to determine experience. Putting hands on a keyboard and proving that you have talent, aptitude, and experience is another way. But while an interesting and relevant problem, its solution is very broad, qualitative, creative, and subjective. The reality is that we still associate much of a candidate's expertise with a degree, certification, and direct cybersecurity experience. And while some CISOs are creative with finding talent,

cybersecurity-related experience is still important to them. Degrees and certifications remain a way to objectively see if someone has "experience." Whether we like it or not, this mindset will not change overnight or within the next few years—and we must work with this reality.

Diversity

Addressing diversity issues within cybersecurity is near and dear to the NTSC. We need a more diverse cyber workforce—especially more women and minorities—to help increase the cybersecurity talent pipeline. Women only represent 24 percent of the cybersecurity workforce, only six percent of the STEM workforce are African-American, and only seven percent of the STEM workforce are Hispanic.

Diversity issues impact the cybersecurity workforce shortage by lessening the number of people interested in the industry. Women and minorities do not see enough role models to envision a cybersecurity career path for themselves, and many candidates are dissuaded from entering the industry. In an NTSC CISO Conversation, Elizabeth Joyce, CISO of State Street, says, "We need to minimize barriers and encourage more women and underrepresented minorities to join the field. And it must feel like an equal playing field regarding pay, treatment, and respect."

In another NTSC CISO Conversation, Selim Aissi, CSO of Ellie Mae, adds, "Work environments must operate slightly different to encourage the hiring and retention of a diverse workforce, and a company's culture must appeal to different groups. The key to diversity is making sure a company's culture accommodates a diverse workforce and provides a clear career development plan so that employees have a clear career path within the organization and are incentivized to work hard to achieve it."

In an NTSC interview, Aric Perminter, Board Member for the International Consortium of Minority Cybersecurity Professionals (ICMCP), said CISOs need to do three things: "Be more creative about where they search for their workforce, clearly articulate growth opportunities within the company to potential new employees, and relax some of the hiring criteria aligned with the job role that's placed on candidates."

As we can see from CISOs and experts on diversity such as Perminter, diversity is a long-term problem needing creativity about hiring, awareness about career paths within companies, and relaxed hiring criteria. This strategy should not only apply to minority candidates but also be implemented broadly across the workforce. However, diversity can also be tackled partially and more concretely in the short-term through making it easier for women and minorities to enter the cybersecurity workforce—such as through cyber scholarship for service programs, as we will discuss below—that can make it easier to select diverse candidates as part of an organization's hiring program.

Why We Need a Pipeline of Experienced Candidates, Now!

It's one thing to look at supply and demand numbers to see the shortage of experienced candidates. It's another thing to ask why the cybersecurity industry needs more immediately experienced candidates. After all, many other industries must work through similar problems of supply and demand, and we all wish candidates were as experienced as we'd like them.

This lack of experienced cybersecurity industry candidates is critically important for a few reasons.

- **It takes years for inexperienced cybersecurity employees to provide value in an environment where threats evolve rapidly and companies need people now**: According to many CISOs, it generally takes up to two years for an entry-level cybersecurity employee to become truly valuable to an organization. In cybersecurity time, that's an eternity, especially because companies' cybersecurity demands are so pressing and the terrain changes so rapidly. For a long-term strategy, companies need to work hard at growing their workforces from the bottom. In such fast-paced environments, these entry-level candidates will make mistakes but receive the opportunity to gain experience, under fire, with experienced mentors. However, it's clear that relying only on entry-level candidates is not enough of a short-term solution.

- **Cybersecurity is an unusual, rapidly evolving new field without a developed talent pipeline going back many decades**: As Marene Allison, CISO of Johnson and Johnson, said in a recent podcast, if someone says they have more than 20 years of cybersecurity experience, she's skeptical. Cybersecurity is still such a new field that a pipeline of experienced candidates hasn't developed like older industries such as financial services or healthcare. Plus, many experienced cybersecurity candidates found their way into security by way of IT, compliance, the military, and other areas rather than through a clear-cut cybersecurity career path. Cybersecurity degree programs are also still relatively new, and newer specialized fields such as penetration testing or cloud security just don't have enough experienced candidates to fill positions.
- **Without a pipeline, security teams are overworked, stressed, fatigued, and over-reliant on vendors**: Studies and surveys show that overwork and fatigue are serious problems with security teams. 65 percent of cybersecurity analysts consider quitting due to burnout, 42 percent of CISOs have given up on proactive cybersecurity, and alert fatigue continues to increase. When there are not enough people able to handle cybersecurity workloads, then security teams must focus on the urgent, possibly weaken their security measures, and overly rely on third party vendors.
- **A retirement wave looms:** The precious few experienced cybersecurity professionals will retire in a wave. 50 percent of the cybersecurity workforce consists of Baby Boomers and Gen Xers who will retire over the next few years. This exodus is already beginning, worsening the cybersecurity talent pipeline at a crucial time. We need experienced, seasoned professionals to staunch the bleeding that companies will face as these people retire.

The Case for Cyber Scholarship for Service Programs

Four-year colleges and certifications are not enough to quickly develop experienced talent. Colleges and universities promote the need for degrees, vendors promote the need for certifications, and HR departments prefer the measurability those degrees and certifications provide. However, practitioners need experienced talent now and tell us candidates don't necessarily need a specific degree or certification—just the experience.

With the help of the federal government, the NTSC recommends and supports scaling up two programs to quickly create a pipeline of more experienced cybersecurity professionals, ready to work for companies when they are hired.

Apprenticeships

In the UK, students receive the General Certificate of Secondary Education at age 16 and then make a decision: Study for the A Level (which means two more years in school and then usually going on to college or university) or leave school to enter into an apprenticeship. To learn a trade, apprentices spend up to six years receiving on-the-job-training while studying. A UK public-private partnership funds apprenticeship programs to help create a needed workforce for trade professions while acknowledging the reality that not everyone needs a university degree to make a living.

Such a public-private apprenticeship program is perfect for cybersecurity. Currently, a few efforts (such as The Cyber Ready Workforce Act that focuses on grants for apprenticeships around certifications) are limited and focused on certifications. Instead, real-world on-the-job training as part of an apprenticeship program, giving students years of work experience, is perfect for supplying the cybersecurity industry with much-needed experienced talent. To do this, we must acknowledge that college is not the only path to a cybersecurity career.

However, we cannot leave this process to a handful of grants and isolated efforts. We need a partnership between the federal government and the private sector to create a groundswell of cybersecurity apprenticeships. Students out of high school would work for companies, receiving on-the-job training and study over a period of years. Once they leave the apprenticeship program, their years of work experience make them more valuable to employers on day one.

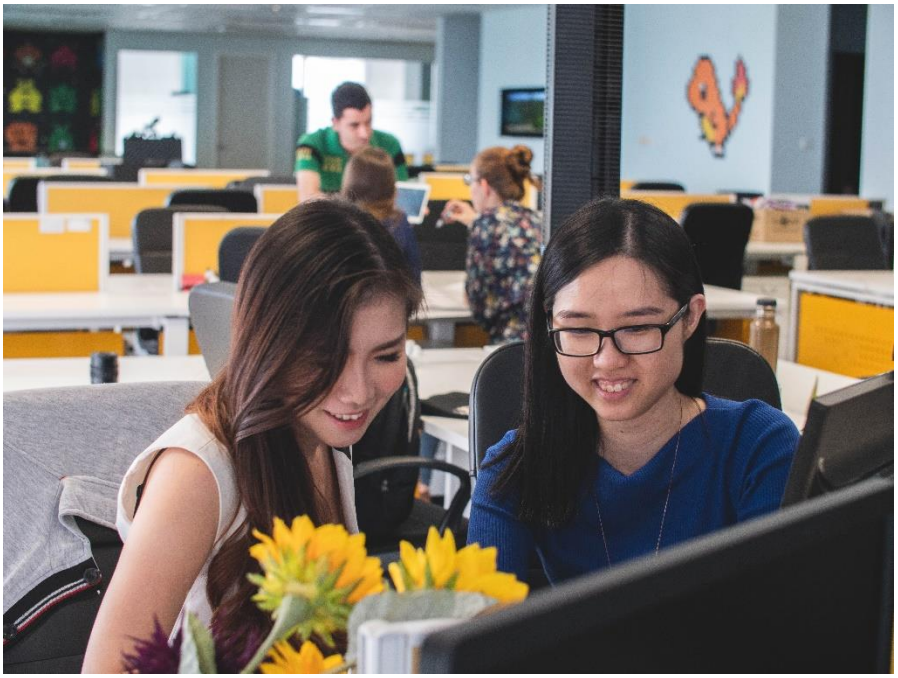
Cyber Scholarship for Service Programs

Federal-funded apprenticeships will help increase the supply of experienced talent by developing the skills of high school students not destined for colleges or universities. But what about the many college students aiming for four-year degrees who unwittingly saturate the market with inexperienced talent? Cyber scholarship for service programs may provide the answer.

Unlike apprenticeships, the CyberCorps® Scholarship for Service Program (SFS) requires that cybersecurity graduates work up to three years for the federal government, equaling the length of the scholarship that funded their college education. Since the program began in 2001, 3,600 graduates have been placed in federal government cybersecurity jobs. Its diversity is not particularly great (25 percent women, 12 percent Asian, 10 percent African American), but its placement rate for candidates ranged between 92 and 95 percent.

Currently, only 86 participating institutions across 29 states exist. Even highly populous states only have a handful of institutions offering the SFS program (Texas with eight, California with four, and New York with four). While 86 is a great start, we need nearly every college and university that offers a cybersecurity degree program to become part of SFS.

A similar program is the Cybersecurity Talent Initiative, which places undergraduate and graduate students in a federal agency for two years. In return, students receive up to $50,000 in student loan assistance and an opportunity to apply for positions at private sector companies that partner with the Cybersecurity Talent Initiative. Partners include Mastercard, Microsoft, Workday, and CyberVista.



The Case for Expanding Both Apprenticeship and Cyber Scholarship for Service Programs

A few compelling reasons exist for vastly expanding apprenticeship programs and the SFS program.

- **These programs will give students, apprentices, and entry-level candidates experience**: By working as an apprentice or for the federal government, students earn invaluable experience in real-world scenarios. This training, as part of a funded program, gives entry-level candidates as much as three to six years of experience as a jumpstart to their career.
- **These programs will supply the public sector with desperately needed workforce talent**: The SFS program allows the federal government to fund and acquire a talent pipeline that provides a much-needed pool of talent. It's also a chance to compete with the private sector. Because a person will work for the federal government for one to three years, they will get a tangible sense of what it's really like to work for an agency, see the benefits they receive, and possibly grow acculturated to their role. This increases the likelihood of both securing and retaining talented people who otherwise would graduate from college and pass the government by without a thought. Graduates also have lots of options: state government, federal government, the FBI, US Cyber Command, Army Command, or other agencies.
- **These programs will supply the private sector with experienced workforce talent**: Conversely, many people will not stay with the public sector after their SFS service is over. Instead of entry-level talent, the private sector will receive resumes from apprentices and SFS graduates with, on average, two or more years of experience. Apprentices and SFS graduates create a large pool of talent who are productive on day one.

Scaling Up Apprenticeships and SFS Programs: What We Need to Supply Our Workforce with Cybersecurity Talent

We are not starting from scratch. To date, Congress, the federal government, and the private sector have attempted apprenticeships and SFS programs in a piecemeal fashion. These efforts include:

- **Limited apprenticeship programs:** Congress so far has mostly focused on grants for cybersecurity apprenticeships around certifications, replicating the issue of entry-level certifications not addressing the core cybersecurity talent shortage. Other limited programs include initiatives such as the Cybersecurity Apprenticeship Program in North Carolina (focused on veterans), experimentation as part of NICE's strategic plan, and a smattering of colleges and universities that have implemented apprenticeship programs. While these programs and grants are a fantastic start, they have limited impact and are not widely accessible or funded.
- **Limited private sector programs:** As an example, the Cybersecurity Talent Initiative mentioned earlier is an excellent, best-of-breed private sector program. However, right now only five companies are participating in this program and the initiative funds up to 5 people per company. That's only 25 people. While a great forward-looking idea, we need to expand and scale it so that many more companies can get involved across the nation.
- **Too few SFS participating institutions**: 86 institutions are better than zero, but it's still far too few in a country with over 5,000 colleges and universities—with many of these higher education institutions offering cybersecurity degree programs. We need to get more colleges and universities qualified for the SFS program. According to the SFS website, "The process for a university to participate in the Cyber Corps®: Scholarship for Service (SFS) program is a competitive one. […] While several institutions apply each year, only a few are selected." This approach is simply unacceptable in an environment where we need to develop and supply as much cybersecurity talent as possible. It's ridiculous to think that only 86 colleges and universities in a sea of over 5,000 are currently capable of providing SFS candidates to a public sector experiencing critical talent shortages. If a college or university meets a certain criteria and has a nationally recognized cybersecurity program, then they should be able to graduate people who then have the option of going into the federal government for up to three years and getting a percentage of their student debt forgiven. While it's important to maintain quality control, the program needs to be more creative and flexible in view of the state of the cybersecurity workforce and where it needs to go.

To scale up and expand these programs so that we supply more cybersecurity talent to the private and public sectors, the NTSC recommends the following:

- **Fund a national cybersecurity apprenticeship program:** Like the UK, the US needs to fund a national cybersecurity apprenticeship program that allows high school students to gravitate to cybersecurity like a trade. If they show interest and aptitude, they can train on the job while studying cybersecurity. The time period, like the UK, may be up to six years. By offering this program nationwide, we will widely expand the cybersecurity workforce beyond four-year degree graduates and provide both the public and private sectors with experienced talent.
- **Expand the SFS program nationally**: The SFS program already exists and simply needs to be expanded to many, many more colleges and universities. Congressional leaders can develop a bill that supports a broader version of the SFS program. The CSC report suggests that we can possibly turn out 2,000 SFS students each year.
- **Improve the security clearance process:** We need to speed up the security clearance process and start the process earlier. Often, candidates who have been through SFS sit for a year or more while the security clearance process plays out. For example, an initiative with Cyber Florida to start the clock early on the clearance process has the potential to help if the Defense Counterintelligence and Security Agency (DCSA) can adapt quickly enough.
- **Scale up successful pilot programs and limited initiatives**: If programs work on a more limited basis, then we need to expand these programs—whether as part of an apprenticeship program, the SFS program, or a separate national program. For example, can the Mastercard program be merged into the SFS program? Can the North Carolina apprenticeship program become part of a national program? Can we model a national program based on successful public-private partnership programs run by various colleges and universities? We need national coordination from NICE or another federal agency to detail and analyze existing elements of successful programs. What elements work? Is there any confusion between programs that can get resolved? What should an apprentice or SFS program candidate get (such as tuition paid off, no college debt, payments suspended while in the program, etc.)?
- **Scale up training and retraining programs**: Within companies, identifying non-traditional candidates who may work for other departments and show an interest in cybersecurity need access to training and retraining programs. Similarly, publicly funded training and retraining programs to help experienced mid-career professionals' transition into cybersecurity may also produce more talented candidates. As many CISOs note, some of the most talented members of their team come from non-cybersecurity career paths.

Conclusion

It's possible the pandemic and resulting recession may make the cybersecurity workforce shortage irrelevant. Looking further ahead over the next 3-5 years, the cyber workforce may shrink due to AI, machine learning, automation, and orchestration. This entire problem could go away. As digital transformation continues to revolutionize companies, industries, and the economy, the 2020s may prove transformational on cybersecurity as well as the business models of companies.

However, not only is it too early to know for sure how these events, trends, and impacts will play out, we will continue to need human minds behind the AI and machines to help us outthink our adversaries. China, Russia, Iran, and North Korea will continue to throw minds behind the development of their cybersecurity programs to further their national interests while disrupting ours.

A national investment in cybersecurity apprenticeships and cyber scholarship for service programs fills an important gap in our talent pipeline. As we focus long-term on developing the next generation of our cybersecurity workforce, as we confront problems related to K-12 cybersecurity evangelism and diversity, and as we reimagine the hiring processes for cybersecurity candidates, we also need a short-term solution that helps the public and private sector get experienced candidates now.

Congress can pass legislation that scales up existing programs that work, invests in our cybersecurity workforce in innovative ways, and amplifies our talent pipelines in a way that makes us more competitive globally and improves our national security. It is imperative, nonpartisan, and uncontroversial for legislators to prioritize working across the aisle to pass a law enacting a national apprenticeship and cyber scholarship for service program.

To learn more about the NTSC, visit us at ntsc.org.